

National Yang Ming Chiao Tung University Regulations

Governing Information Security and Personal Information Protection

Approved at the fifth Administrative Meeting for the 2020–2021 academic year on June 2, 2021.

1. To maintain information security and protect personal information, National Yang Ming Chiao Tung University (hereinafter referred to as “the University”) established the National Yang Ming Chiao Tung University Regulations Governing Information Security and Personal Information Protection (hereinafter referred to as “the Regulations”) to enhance security management for information assets; ensure the confidentiality, integrity, availability, distinguishability, and non-repudiation of these assets; and support faculty and students in ensuring the protection of their personal information with respect to the application of information systems to meet specific operation demands.
2. The Regulations, including ancillary requirements established based on them, were created by referencing the Cyber Security Management Act, the Personal Data Protection Act, the Copyright Act, and the Classified National Security Information Protection Act; information security management regulations established by the Executive Yuan and affiliated agencies; Directions Governing Information Security in Educational System; and other relevant regulations and standards.
3. The Regulations apply for all informational assets and information users associated with the University. Information users must adhere to the Regulations; those who violate the Regulations shall be penalized according to relevant laws.
4. The Vice-President of the University shall be appointed by the President to serve as the Information Security Manager and shall be responsible for supervising the implementation of information security and personal data protection policies in the University. Additionally, an executive secretary shall be appointed to assist the Information Security Manager in this regard.
5. To ensure that the information security and personal data protection tasks of the University are executed, an Information Security and Personal Data Protection Committee (hereinafter referred to as the “the Committee”) shall be established as an interdisciplinary division. The Committee is responsible for the planning, coordinating, and drafting of information security and personal data protection policies and plans, as well as resource allocation and the execution of relevant tasks. The Committee members shall comprise the Vice-President, Secretary General, Dean of Academic Affairs, Dean of Student Affairs, Dean of General Affairs, Dean of Research and Development, Dean of International Affairs, Curator, Director of the Center of Environmental Protection and Safety and Health, Director of the Personnel Office, and Director of the Accounting Office, as well as one representative from NCYU

School of Law and the Director of the IT Service Center, who shall be appointed as the ex officio committee member. The Committee members shall convene for at least one management and evaluation meeting annually, with the Information Security Manager serving as the convenor.

6. The University shall establish an Information Security and Personal Data Protection Task Group. The members of this group shall comprise senior operators of the IT Service Center, individuals in charge of core operational tasks, and second-level executives of core operational divisions. This task group shall be responsible for the planning, execution, and auditing of information security and personal data protection operational principles. The Director of the IT Service Center shall serve as the convener of this task group.
7. In accordance with the Cyber Security Management Act and Personal Data Protection Act, the IT Service Center shall establish the National Yang Ming Chiao Tung University Cyber Security Management Act and Personal Data Protection Implementation Regulations to govern policies, goals, and core operations related to information security and personal data protection. The regulations shall be implemented after approval by the Committee, and the same rule shall apply to all subsequent amendments.
8. The University shall conduct information security and personal data protection education training and promotion to improve faculty and students understanding of information security and personal data protection.
9. The Regulations shall be reviewed regularly to reflect the most recent relevant standards, technologies, and operational conditions.
10. The Regulations shall be implemented after approval by the attendees of the Administrative Meeting. The same rule shall apply to all subsequent amendments.